PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-273936
(43)Date of publication of application : 26.09.2003

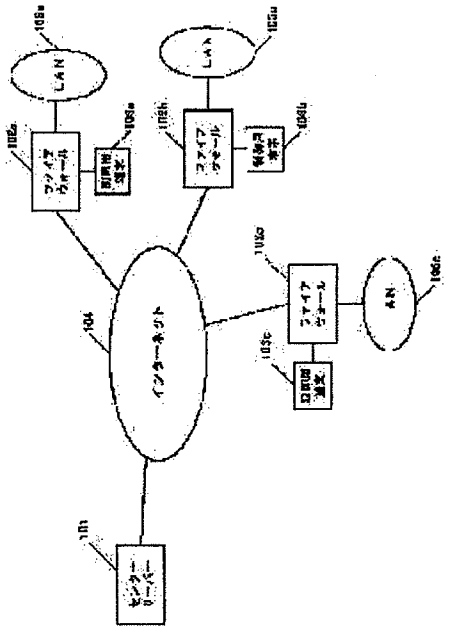
(51)Int.Cl. H04L 12/66
G06F 13/00

(21)Application number : 2002-072754
(22)Date of filing : 15.03.2002

(71)Applicant : FIRST TRUST:KK
(72)Inventor : FUKUSHIRO SHIGEO
ARAKI MASAYUKI

(54) FIREWALL SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a packet filtering type firewall system which is easily operated.
SOLUTION: Each firewall device 102 performs packet filtering according to prescribed filtering rules, further monitors a packet which can be passed by the present filtering rules and, when the packet is judged to be refused, extracts a transmitting origin IP address from the header part of the packet and updates the filtering rules on the basis of extracted information. Furthermore, the transmitting origin IP address, etc., are recorded and periodically transmitted to a maintenance center server 101. The server 101 periodically processes the information transmitted from each device 102 statistically and transmits a refused IP address, etc., which is judged to be shared by a plurality of the devices 102 to each device 102. Each device 102 updates the filtering rules of itself, etc., on the basis of the information transmitted from the server 101.



[0002]

[Conventional Art] Conventionally, as a technology for ensuring network security, a firewall has been known. The firewall is placed between an external network such as Internet and an internal network such as an in-enterprise LAN and is a technique for blocking such as an intrusion from the external network to the internal network by controlling whether to permit communication for every data based on a predefined standard.

[0003] Such a firewall has various systems, among which, a packet filtering type firewall system is available. The packet filtering type firewall system controls whether to permit passing of every packet from an external network to an internal network (or an internal network to an external network). Such a control is performed in accordance with a predetermined filtering rule.

[0004] Normally, under the filtering rule, a packet to be a filtering target is identified by a transmission source IP address, a destination IP address, a transmission source port number, a destination port number, type of protocol, and the like and an action (pass, rejection, etc.) for the packet is designated.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2003－273936
（P2003－273936A）
(43)公開日　平成15年９月26日(2003.9.26)

(51)Int.Cl.[7]	識別記号	ＦＩ	テーマコード(参考)
Ｈ０４Ｌ　12/66		Ｈ０４Ｌ　12/66	Ｂ　５Ｂ０８９
Ｇ０６Ｆ　13/00	３５１	Ｇ０６Ｆ　13/00	３５１Ｚ　５Ｋ０３０

審査請求　未請求　請求項の数13　ＯＬ　（全 14 頁）

(21)出願番号　特願2002－72754(P2002－72754)

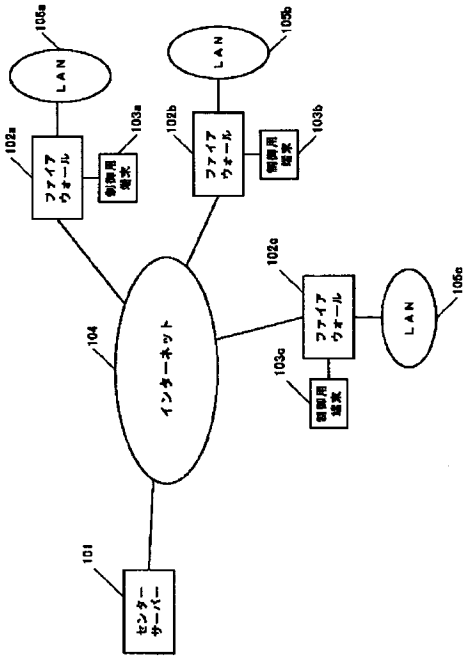
(22)出願日　平成14年３月15日(2002.3.15)

(71)出願人　502094354
株式会社ファーストトラスト
広島県広島市安佐南区長東西五丁目２番13号
(72)発明者　福城　茂生
広島県広島市安佐南区長東西五丁目２番13号　株式会社ファーストトラスト内
(72)発明者　荒木　正之
広島県広島市安佐南区長東西五丁目２番13号　株式会社ファーストトラスト内
(74)代理人　100111084
弁理士　藤野　義昭

最終頁に続く

(54)【発明の名称】　ファイアウォールシステム

(57)【要約】
【課題】　運用するのが容易なパケットフィルタリング型のファイアウォールシステムを提供する。
【解決手段】　各ファイアウォール装置102は、所定のフィルタリングルールに従ってパケットフィルタリングを行い、更に、現在のフィルタリングルールでは通過可能なパケットを監視し、当該パケットを拒否すべきと判定した場合は、当該パケットのヘッダ部から送信元ＩＰアドレスを抽出し、抽出した情報に基づいてフィルタリングルールの更新を行う。更に、その送信元ＩＰアドレス等を記録しておき、定期的に保守センターサーバー101に送信する。サーバー101は、各装置102から送られてくる情報を定期的に統計処理し、複数の装置102で共有すべきと判断される拒否ＩＰアドレス等を、各装置102へ送信する。各装置102は、サーバー101から送られてきた情報に基づいて、自己のフィルタリングルール等を更新する。



1

【特許請求の範囲】

【請求項１】　保守センターサーバーと、複数のファイアウォール装置とが、ネットワークを介して接続されたファイアウォールシステムであって、

各ファイアウォール装置は、

自己が保持するフィルタリングルールに基づいて、パケットのフィルタリングを行うとともに、自己が受信したパケットに基づいて、当該パケットを拒否すべきか否かを判定し、拒否すべきと判定した場合は、当該パケットを拒否できるように、前記フィルタリングルールを更新し、

また、拒否すべきと判定したパケットに関する拒否パケット情報を保守センターサーバーへ送信し、

保守センターサーバーは、

各ファイアウォール装置から送られてくる拒否パケット情報を統計処理して、複数のファイアウォール装置で共有すべき拒否パケット識別情報を決定し、

複数のファイアウォール装置で共有すべき拒否パケット識別情報を、各ファイアウォール装置に送信し、

各ファイアウォール装置は、保守センターサーバーから送られてきた拒否パケット識別情報に基づいて、フィルタリングルールを更新することを特徴とするファイアウォールシステム。

【請求項２】　保守センターサーバーと、複数のファイアウォール装置とが、ネットワークを介して接続されたファイアウォールシステムであって、

各ファイアウォール装置は、自己の動作モード情報を保守センターサーバーへ送信し、

保守センターサーバーは、各ファイアウォール装置から送られてきた動作モード情報に合致する拒否パケット識別情報を、各ファイアウォール装置に送信し、

各ファイアウォール装置は、保守センターサーバーから送られてきた拒否パケット識別情報に基づいて、フィルタリングルールを生成し、当該フィルタリングルールに基づいて、パケットのフィルタリングを行うことを特徴とするファイアウォールシステム。

【請求項３】　フィルタリングルールに基づいて、パケットの通過を許可するか否かを制御するパケットフィルタリング部と、パケットを捕捉し、捕捉したパケットから必要な情報を抽出するパケット捕捉部と、

前記パケット捕捉部が抽出した情報に基づいて、捕捉したパケットが拒否すべきパケットであるか否かを判定し、拒否すべきパケットであると判定した場合、当該パケットから、フィルタリングルールを生成するのに必要な情報を抽出する判定部と、

当該判定部が抽出した情報に基づいて、前記フィルタリングルールを更新するルール更新部とを備えたことを特徴とするファイアウォール装置。

【請求項４】　前記判定部は、

パケットのデータに、予め決められた文字列が含まれているか否かによって、拒否すべきパケットであるか否かを判定することを特徴とする請求項３に記載のファイアウォール装置。

2

【請求項５】　前記判定部は、

所定の時間内に、同一の送信元から所定数以上のメール・パケットを受信したか否か、及び、当該パケットが転送メールに関連するパケットであるか否かによって、拒否すべきパケットであるか否かを判定することを特徴とする請求項３に記載のファイアウォール装置。

【請求項６】　前記判定部は、

所定の時間内に、同一の送信元から所定の複数のポートに対するアクセスがあったか否かによって、拒否すべきパケットであるか否かを判定することを特徴とする請求項３に記載のファイアウォール装置。

【請求項７】　前記ルール更新部は、フィルタリングルールを更新した場合、当該フィルタリングルールを更新するのに必要な情報と、更新を行った原因と、更新を行った時刻を記録し、

当該記録を、外部ネットワークを介して、保守センターサーバーへ送信するデータ送信部を更に備えることを特徴とする請求項３～６のいずれか一項に記載のファイアウォール装置。

【請求項８】　前記ルール更新部は、フィルタリングルールを追加した場合、追加を行った時刻を記録しておき、その時刻から所定の時間が経過した後、追加したフィルタリングルールを削除することを特徴とする請求項３～６のいずれか一項に記載のファイアウォール装置。

【請求項９】　保守センターサーバーから送られてくる拒否パケット識別情報を受信するデータ受信部を更に備え、

前記ルール更新部は、前記拒否パケット識別情報に基づいて、前記フィルタリングルールを更新することを特徴とする請求項３～８のいずれか一項に記載のファイアウォール装置。

【請求項１０】　保守センターサーバーから送られてくる拒否パケット識別情報を受信するデータ受信部を更に備え、

前記ルール更新部は、前記拒否パケット識別情報に基づいて、前記フィルタリングルールを更新し、

前記判定部は、前記拒否パケット識別情報に含まれる拒否文字列に基づいて、拒否すべきパケットであるか否かを判定することを特徴とする請求項４に記載のファイアウォール装置。

【請求項１１】　パケットフィルタリングのためのフィルタリングルールを生成するプログラムであって、コンピュータをパケットを捕捉し、捕捉したパケットから必要な情報を抽出するパケット捕捉手段、

前記パケット捕捉手段が抽出した情報に基づいて、捕捉したパケットが拒否すべきパケットであるか否かを判定し、拒否すべきパケットであると判定した場合、当該パ

ケットからフィルタリングルールを生成するのに必要な情報を抽出する判定手段、及び当該判定手段が抽出した情報に基づいて、前記フィルタリングルールを生成するフィルタリングルール生成手段として機能させるためのプログラム。

【請求項１２】　ファイアウォール装置から送られてくる拒否パケット情報を受信するデータ受信部と、
受信した拒否パケット情報を記録する記録部と、
記録された拒否パケット情報の統計処理を行う統計処理部と、
前記統計処理された情報から生成される拒否パケット識別情報を格納するデータベースと、
前記データベースに格納された拒否パケット識別情報を、ファイアウォール装置に送信するデータ送信部とを備えたことを特徴とする保守センターサーバー。

【請求項１３】　前記ファイアウォール装置から送られてくる情報には、当該ファイアウォール装置の動作モード情報が含まれ、
当該動作モード情報に基づいて、前記データベースに格納された拒否パケット識別情報を選択し、データ送信部に渡す選択部を更に備えることを特徴とする請求項１２に記載の保守センターサーバー。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、外部ネットワークと内部ネットワークの間で、パケットフィルタリングを行うファイアウォールシステムに関する。

【０００２】

【従来の技術】従来から、ネットワークセキュリティを確保するための技術として、ファイアウォールが知られている。ファイアウォールとは、インターネット等の外部ネットワークと、企業内ＬＡＮ等の内部ネットワークとの間に置かれ、予め決められた基準に基づいて、各データについて通信を許可するか否かを制御することにより、外部ネットワークから内部ネットワークへの侵入等を阻止するための技術である。

【０００３】このようなファイアウォールには、様々な方式のものがあるが、そのうちの一つに、パケットフィルタリング型のファイアウォールがある。パケットフィルタリング型のファイアウォールは、パケット毎に、外部ネットワークから内部ネットワークへの（又は、内部ネットワークから外部ネットワークへの）通過を許可するか否かの制御を行うものであり、このような制御は、予め決められたフィルタリングルールに従って行われる。

【０００４】通常、フィルタリングルールでは、送信元ＩＰアドレス、宛先ＩＰアドレス、送信元ポート番号、宛先ポート番号、プロトコルの種類等によってフィルタリングの対象にするパケットが特定され、当該パケットに対する処置（通過、拒否等）が指定される。

【０００５】

【発明が解決しようとする課題】このようなフィルタリングルールは、管理者が予め設定する必要があるが、その設定作業には、ある程度のネットワーク等に関する知識が必要となり、一般ユーザには困難であった。また、そのような知識を有する者にとっても煩雑であった。

【０００６】本発明の目的は、運用するのが容易なパケットフィルタリング型のファイアウォールシステムを提供することにある。

【０００７】

【課題を解決するための手段】本発明に係るファイアウォールシステムは、保守センターサーバーと、複数のファイアウォール装置とが、ネットワークを介して接続されたファイアウォールシステムである。

【０００８】そして、第一のファイアウォールシステムにおいては、各ファイアウォール装置は、自己が保持するフィルタリングルールに基づいて、パケットのフィルタリングを行うとともに、自己が受信したパケットに基づいて、当該パケットを拒否すべきか否かを判定し、拒否すべきと判定した場合は、当該パケットを拒否できるように、前記フィルタリングルールを更新し、また、拒否すべきと判定したパケットに関する拒否パケット情報を保守センターサーバーへ送信する。保守センターサーバーは、各ファイアウォール装置から送られてくる拒否パケット情報を統計処理して、複数のファイアウォール装置で共有すべき拒否パケット識別情報を決定し、複数のファイアウォール装置で共有すべき拒否パケット識別情報を、各ファイアウォール装置に送信する。そして、各ファイアウォール装置は、保守センターサーバーから送られてきた拒否パケット識別情報に基づいて、フィルタリングルールを更新する。

【０００９】また、第二のファイアウォールシステムにおいては、各ファイアウォール装置は、自己の動作モード情報を保守センターサーバーへ送信する。保守センターサーバーは、各ファイアウォール装置から送られてきた動作モード情報に合致する拒否パケット識別情報を、各ファイアウォール装置に送信する。そして、各ファイアウォール装置は、保守センターサーバーから送られてきた拒否パケット識別情報に基づいて、フィルタリングルールを生成し、当該フィルタリングルールに基づいて、パケットのフィルタリングを行う。

【００１０】本発明に係るファイアウォール装置は、フィルタリングルールに基づいて、パケットの通過を許可するか否かを制御するパケットフィルタリング部と、パケットを捕捉し、捕捉したパケットから必要な情報を抽出するパケット捕捉部と、前記パケット捕捉部が抽出した情報に基づいて、捕捉したパケットが拒否すべきパケットであるか否かを判定し、拒否すべきパケットであると判定した場合、当該パケットから、フィルタリングルールを生成するのに必要な情報を抽出する判定部と、当

該判定部が抽出した情報に基づいて、前記フィルタリングルールを更新するルール更新部とを備えたことを特徴とする。

【００１１】この場合において、前記判定部は、パケットのデータに、予め決められた文字列が含まれているか否かによって、拒否すべきパケットであるか否かを判定するようにしてもよい。また、所定の時間内に、同一の送信元から所定数以上のメール・パケットを受信したか否か、及び、当該パケットが転送メールに関連するパケットであるか否かによって、拒否すべきパケットであるか否かを判定するようにしてもよい。また、所定の時間内に、同一の送信元から所定の複数のポートに対するアクセスがあったか否かによって、拒否すべきパケットであるか否かを判定するようにしてもよい。

【００１２】また、前記ルール更新部は、フィルタリングルールを更新した場合、当該フィルタリングルールを更新するのに必要な情報と、更新を行った原因と、更新を行った時刻を記録するようにしてもよく、そして、前記ファイアウォール装置が、当該記録を、外部ネットワークを介して、保守センターサーバーへ送信するデータ送信部を更に備えるようにしてもよい。

【００１３】また、前記ルール更新部は、フィルタリングルールを追加した場合、追加を行った時刻を記録しておき、その時刻から所定の時間が経過した後、追加したフィルタリングルールを削除するようにしてもよい。

【００１４】また、前記ファイアウォール装置が、保守センターサーバーから送られてくる拒否パケット識別情報を受信するデータ受信部を更に備え、前記ルール更新部が、前記拒否パケット識別情報に基づいて、前記フィルタリングルールを更新するようにしてもよい。

【００１５】また、前記判定部が、パケットのデータに、予め決められた文字列が含まれているか否かによって、拒否すべきパケットであるか否かを判定する場合は、ファイアウォール装置が、保守センターサーバーから送られてくる拒否パケット識別情報を受信するデータ受信部を更に備え、前記ルール更新部は、前記拒否パケット識別情報に基づいて、前記フィルタリングルールを更新し、前記判定部は、前記拒否パケット識別情報に含まれる拒否文字列に基づいて、拒否すべきパケットであるか否かを判定するようにしてもよい。

【００１６】本発明に係るパケットフィルタリングのためのフィルタリングルールを生成するプログラムは、コンピュータを、パケットを捕捉し、捕捉したパケットから必要な情報を抽出するパケット捕捉手段、前記パケット捕捉手段が抽出した情報に基づいて、捕捉したパケットが拒否すべきパケットであるか否かを判定し、拒否すべきパケットであると判定した場合、当該パケットからフィルタリングルールを生成するのに必要な情報を抽出する判定手段、及び、当該判定手段が抽出した情報に基づいて、前記フィルタリングルールを生成するフィルタリングルール生成手段として機能させるためのプログラムである。

【００１７】本発明に係る保守センターサーバーは、ファイアウォール装置から送られてくる拒否パケット情報を受信するデータ受信部と、受信した拒否パケット情報を記録する記録部と、記録された拒否パケット情報の統計処理を行う統計処理部と、前記統計処理された情報から生成される拒否パケット識別情報を格納するデータベースと、前記データベースに格納された拒否パケット識別情報を、ファイアウォール装置に送信するデータ送信部とを備えたことを特徴とする。

【００１８】この場合において、前記ファイアウォール装置から送られてくる情報には、当該ファイアウォール装置の動作モード情報が含まれるようにしてもよく、そして、前記保守センターサーバーが、当該動作モード情報に基づいて、前記データベースに格納された拒否パケット識別情報を選択し、データ送信部に渡す選択部を更に備えるようにしてもよい。

【００１９】

【発明の実施の形態】以下、本発明の実施の形態について、図面を参照しつつ詳細に説明する。

【００２０】図１は、本発明によるファイアウォールシステムの全体構成を示す図である。

【００２１】同図に示すように、本システムは、保守センターサーバー１０１と、複数のファイアウォール装置１０２（１０２ａ～１０２ｃ）と、複数の制御用端末装置１０３（１０３ａ～１０３ｃ）とを備える。

【００２２】保守センターサーバー１０１及びファイアウォール装置１０２は、共に、インターネット１０４に接続されている。また、各ファイアウォール装置１０２は、それぞれ、内部ネットワーク１０５（１０５ａ～１０５ｃ）に接続されている。

【００２３】更に、各ファイアウォール装置１０２は、シリアルケーブルを介して、各制御用端末装置１０３と接続されている。制御用端末装置１０３は、ファイアウォール装置１０２の各種設定を行ったり、ファイアウォール装置１０２の状態を確認したりするためのものである。

【００２４】各ファイアウォール装置１０２は、外部ネットワークであるインターネット１０４と内部ネットワーク１０５との間で、パケットフィルタリングを行う。各ファイアウォール装置１０２は、予め決められたフィルタリングルールに従って、パケットフィルタリングを行うが、更に、現在のフィルタリングルールでは通過可能なパケットを監視し、当該パケットを通過させるのが望ましいか否かを判断する。そして、通過させるのが望ましくないと判定した場合は、当該パケットから、フィルタリングルールを生成するのに必要な情報（例えば、送信元ＩＰアドレス）を抽出し、抽出した情報に基づいて、当該パケットを拒否（遮断）できるようにフィルタ

リングルールの更新を行う。

【００２５】フィルタリングルールを生成するのに必要な情報としては、送信元ＩＰアドレス（又は、ドメイン名）、送信元ポート番号、宛先ＩＰアドレス（又は、ドメイン名）、宛先ポート番号、プロトコル種類等があるが、以下では簡単のため、送信元ＩＰアドレスで、フィルタリングルールを生成するのに必要な情報を代表させる。

【００２６】本実施形態においては、各ファイアウォール装置１０２は、現在は通過可能なパケットに対して、３種類の判定を行う。

【００２７】まず、第一に、各ファイアウォール装置１０２は、パケットのデータ（アプリケーション層のデータ）に、予め決められた文字列（拒否文字列）が含まれるか否かを判定する。そして、拒否文字列を含むパケットは、拒否すべきパケットであると判定する。

【００２８】このような判定を行うことにより、例えば、教育機関のＬＡＮ環境において、児童の目に触れさせたくない文字列（猥褻な言葉や差別用語等）を含むＨＴＭＬファイル等が児童が使う端末装置に表示されるのを防ぐことが可能になる。

【００２９】第二に、各ファイアウォール装置１０２は、パケットが、スパムメールに関連するパケットであるか否かを判定する。スパムメールとは、不特定多数のユーザーに、一方的に送りつけられる宣伝メール等の電子メールのことをいい、多くの場合、電子メールの不正中継が利用される。このようなスパムメールに関連するパケットについては、拒否することが望ましいので、各ファイアウォール装置１０２は、パケットが、スパムメールに関連するパケットであるか否かを判定する。スパムメールに関連するパケットであるか否かを判定する処理の詳細については後述する。

【００３０】第三に、各ファイアウォール装置１０２は、パケットが、ポートスキャンに関連するパケットであるか否かを判定する。一般に、インターネットで利用される多くのサービスは、ＴＣＰ又はＵＤＰのサービスとして、サーバー上で稼働しており、ＴＣＰやＵＤＰにはポート番号と呼ばれるサービス識別子が存在する。ポートスキャンとは、例えば、１番ポートから順番に接続を試みることで、スキャン対象のサーバーで稼働しているサービスが何なのかを調べるものである。このようなポートスキャンに関連するパケットについても、拒否することが望ましいので、各ファイアウォール装置１０２は、パケットが、ポートスキャンに関連するパケットであるか否かを判定する。ポートスキャンに関連するパケットであるか否かを判定する処理の詳細については後述する。

【００３１】各ファイアウォール装置１０２は、以上のような判定の結果、拒否すべきパケットと判定した場合は、当該パケットの送信元ＩＰアドレスを抽出して、抽出した送信元ＩＰアドレスに基づいて、当該送信元ＩＰアドレスからのパケットを拒否できるようにフィルタリングルールを更新する。更に、その際、その送信元ＩＰアドレス、更新原因（拒否文字列検出／スパムメール検出／ポートスキャン検出）、更新時刻等を記録しておき、当該記録（拒否パケット情報）を定期的に、保守センターサーバー１０１に送信する。

【００３２】保守センターサーバー１０１は、各ファイアウォール装置１０２から送られてくる情報を記録し、記録した情報を定期的に統計処理する。そして、統計処理の結果、複数のファイアウォール装置１０２で共有すべきと判断される拒否パケット識別情報（例えば、拒否すべき送信元ＩＰアドレス）を、各ファイアウォール装置１０２へ送信する。

【００３３】各ファイアウォール装置１０２は、保守センターサーバー１０１から送られてくる拒否パケット識別情報を受け取ると、当該情報に基づいて、自己のフィルタリングルール等を更新する。

【００３４】本ファイアウォールシステムでは、このような動作を行うので、各ファイアウォール装置１０２は、現在のフィルタリングルールでは対処できないパケットについても、ある程度、自律的に防御をすることが可能になる。また、あるファイアウォール装置１０２ａにおいて、拒否すべきパケットの送信元と判定された送信元ＩＰアドレスが、他のファイアウォール装置１０２ｂ、１０２ｃでも共用されることとなり、他のファイアウォール装置１０２ｂ、１０２ｃでは、自分で検出しなくても、望ましくないパケットを拒否するようにフィルタリングルールを更新することができ、望ましくないパケットの通過を未然に防ぐことが可能となる。

【００３５】また、各ファイアウォール装置１０２は、自己の動作モード情報の一つとして、カテゴリと呼ばれる情報を有している。カテゴリは、制御用端末装置１０３を使って、管理者が設定（変更）することができる。

【００３６】カテゴリは、例えば、ファイアウォール装置１０２が接続される内部ネットワーク１０５の種類（例えば、「教育機関」、「企業」、「個人」）や、セキュリティレベル（例えば、「高」、「中」、「低」）等に対応して予め定められる識別子（例えば、０００～９９９のいずれか）である。

【００３７】更に、各ファイアウォール装置１０２は、自己の動作モード情報として、「スパムメールをチェックするか否か」、「ポートスキャンをチェックするか否か」の情報を有しており、これらも、制御用端末装置１０３を使って、設定（変更）することができる。

【００３８】各ファイアウォール装置１０２は、これらの動作モード情報が設定あるいは変更されると、当該動作モード情報を保守センターサーバー１０１へ送信する。なお、このとき、前述した拒否パケット情報等が存在すれば、これも同時に送信される。

【００３９】保守センターサーバー１０１は、各ファイアウォール装置１０２から送られてくる動作モード情報を受け取ると、送られてきた動作モード情報に基づいて、当該動作モードに応じた拒否パケット識別情報（本実施形態においては、拒否文字列及び拒否送信元ＩＰアドレス）を選択し、各ファイアウォール装置１０２に送り返す。

【００４０】各ファイアウォール装置１０２は、保守センターサーバー１０１から送られてきた拒否パケット識別情報に基づいて、フィルタリングルールを生成し、また、拒否文字列の判定を行う。

【００４１】本ファイアウォールシステムでは、このような動作を行うので、所望の動作モードを選択するだけで、自己のファイアウォール装置１０２に対して、適切なフィルタリングルール及び拒否文字列を自動的に設定することができ、各ファイアウォール装置１０２の管理者の負担が軽減される。

【００４２】次に、以上のような動作を行う本ファイアウォールシステムを構成する各構成要素の詳細について説明する。

【００４３】まず、ファイアウォール装置１０２の詳細について説明する。

【００４４】図２は、ファイアウォール装置１０２のハードウェア構成例を示す図である。同図に示すように、ファイアウォール装置１０２は、ＣＰＵ２０１と、メインメモリ２０２と、ＲＯＭ２０３と、ＰＣカードインタフェース部２０４と、シリアルインタフェース部２０５と、ネットワークインタフェース部２０６，２０７とを備える。

【００４５】ＣＰＵ２０１、メインメモリ２０２、ＲＯＭ２０３、ＰＣカードインタフェース部２０４、シリアルインタフェース部２０５、ネットワークインタフェース部２０６，２０７は、それぞれ、バス２０８に接続されている。また、ＰＣカードインタフェース部２０４には、フラッシュＡＴＡカード２０９が接続される。シリアルインタフェース部２０５は、制御用端末装置１０３に接続され、ネットワークインタフェース部２０６は、外部ネットワーク（インターネット１０４）に接続され、ネットワークインタフェース部２０７は、内部ネットワーク１０５に接続される。

【００４６】ＣＰＵ２０１は、ファイアウォール装置１０２が行う各種処理を実行・制御する中央処理装置である。メインメモリ２０２は、ＣＰＵ２０１が利用する各種プログラムやデータを格納する主記憶装置である。ＲＯＭ２０３は、ＣＰＵ２０１が利用するＢＩＯＳ等を格納する記憶装置である。

【００４７】ＰＣカードインタフェース部２０４は、フラッシュＡＴＡカード２０９とバス２０８との間のデータのやり取りを制御するものである。シリアルインタフェース部２０５は、制御用端末装置１０３と、バス２０８と間のデータのやり取りを制御するものである。ネットワークインタフェース部２０６は、外部ネットワークとバス２０８との間のデータのやり取りを制御するものである。ネットワークインタフェース部２０７は、内部ネットワークとバス２０８との間のデータのやり取りを制御するものである。

【００４８】フラッシュＡＴＡカード２０９は、ＣＰＵ２０１が利用するオペレーティングシステム（ＯＳ）その他の各種プログラムやデータが記録された記録媒体である。なお、本実施形態においては、フラッシュＡＴＡカードの全記憶領域は、セクタ単位で暗号化が行われている。すなわち、ファイアウォール装置１０２のＯＳ又はＢＩＯＳが、フラッシュＡＴＡカード２０９に対して、セクタ単位で読み書きを行う際、セクタデータに関して所定の復号／符号化を行う。このような処理を行うことにより、例えば、ファイアウォール装置１０２を、ＡＴ互換機等の一般的なパーソナルコンピュータ（ＰＣ）をベースに実現した場合であっても、フラッシュＡＴＡカード２０９に記録された情報が、他の同種のＰＣ等で読み出されることを防止することが可能になる。

【００４９】図３は、ファイアウォール装置１０２のソフトウェア構成例を示す図である。同図に示すように、ファイアウォール装置１０２は、パケットフィルタリング部３０１と、バケット捕捉部３０２と、判定部３０３～３０５と、フィルタリングルール制御部３０６と、データ送信部３０７と、データ受信部３０８とを備える。各部３０１～３０８は、基本的に、ＣＰＵ２０１が、メインメモリ２０２にロードされたプログラムを実行することで実現される。

【００５０】パケットフィルタリング部３０１は、ＴＣＰ／ＩＰプロトコルにおけるＩＰパケットを受け取り、パケットのヘッダの内容に応じて、受け取ったパケットを通過させるか否かの制御を行うものである。パケットフィルタリング部３０１は、フィルタリングルールを保持し、このフィルタリングルールに従って、受け取ったパケットを通過させるか否かを判断する。

【００５１】フィルタリングルール制御部３０６は、パケットフィルタリング部３０１が保持するフィルタリングルールに新たなルールを追加したり、フィルタリングルールからあるルールを削除したりして、フィルタリングルールの制御を行う。

【００５２】パケット捕捉部３０２は、パケットフィルタリング部３０１を通過したパケットを捕捉し、当該パケットの解析を行い、必要なデータを抽出して判定部３０３～３０５に渡す。パケット捕捉部３０２は、また、捕捉したパケットに関する記録を残すため、捕捉パケット記録テーブルを保持している。

【００５３】図４は、捕捉パケット記録テーブルの構成例を示す図である。

【００５４】同図に示すように、捕捉パケット記録テー

ブルは、「送信元」フィールド４０１と、「宛先」フィールド４０２と、「プロトコル」フィールド４０３と、「受信時刻」フィールド４０４とを備えている。

【００５５】「送信元」フィールド４０１には、パケットの送信元のＩＰアドレス（及び、必要に応じてポート番号）が格納される。「宛先」フィールド４０２には、パケットの宛先のＩＰアドレス（及び、必要に応じてポート番号）が格納される。「プロトコル」フィールド４０３には、パケットのプロトコル種別を示す情報が格納される。「受信時刻」フィールド４０４には、パケットを受信した時刻が格納される。

【００５６】パケット捕捉部３０２は、捕捉したパケットのヘッダ部を順次解析し、当該パケットがどのような種類のパケットかを判別する。そして、アプリケーション層のデータ（例えば、ＨＴＭＬファイルの内容）を含むパケットについては、そのデータ部分を、ＴＣＰ／ＩＰヘッダと共に、判定部３０３に送る。また、電子メールに関連するパケットについては、そのメールヘッダを抽出し、ＴＣＰ／ＩＰヘッダと共に、判定部３０４に送る。また、ポートに対してアクセスを行うパケットについては、ＴＣＰ／ＩＰヘッダを判定部３０５に送る。各判定部３０３～３０５は、パケット捕捉部３０２から渡された情報に基づいて、捕捉したパケットが拒否すべきパケットであるか否かを判定する。

【００５７】次に、捕捉したパケットが拒否すべきパケットであるか否かを判定する判定部３０３～３０５について説明する。本実施形態においては、３種類の判定部３０３～３０５が設けられている。

【００５８】まず、判定部３０３について説明する。

【００５９】判定部３０３は、パケットに含まれるアプリケーション層レベルのデータに、予め設定された文字列が含まれているか否かによって、当該パケットが拒否すべきパケットであるか否かを判定する。そのため、判定部３０３は、拒否すべき文字列のリスト（拒否文字列リスト）を保持している。

【００６０】この拒否文字列リストは、ファイアウォール装置１０２の運用開始時に、管理者によって設定されたカテゴリに対応するものが、保守センターサーバー１０１からダウンロードされる。なお、運用開始時の拒否文字列リストについては、予めフラッシュＡＴＡカード２０９に格納しておき、それを利用するようにしてもよい。

【００６１】また、拒否文字列リストには、各ファイアウォール装置１０２を導入したサイト毎に、管理者が所望の文字列を追加等することもできる。そして、この拒否文字列リストは、定期的に（例えば、３日に一回）、他の情報と共に、保守センターサーバー１０１に送られる。更に、拒否文字列リストは、カテゴリ等、各ファイアウォール装置１０２の動作モード情報が変更された場合も、他の情報と共に、保守センターサーバー１０１に送られる。

【００６２】図５は、判定部３０３の判定処理の流れを示すフローチャートである。

【００６３】同図に示すように、判定部３０３は、まず、パケット捕捉部３０２から渡されるＴＣＰ／ＩＰパケットのデータに、拒否文字列リスト内の拒否文字列が存在するか否かを順次、判定する（Ｓ５０１）。

【００６４】その結果、拒否文字列が含まれていなかった場合は（Ｓ５０１：ＮＯ）、そのまま処理を終了する。

【００６５】一方、拒否文字列が含まれていた場合は（Ｓ５０１：ＹＥＳ）、当該パケットを拒否すべきパケットと判定し、当該パケットのヘッダ部から、送信元のＩＰアドレスを抽出する（Ｓ５０２）。そして、判定部３０３は、抽出した送信元ＩＰアドレスと、当該パケットに含まれていた拒否文字列と、判定部３０３を表す識別子を、フィルタリングルール制御部３０６に渡して（Ｓ５０３）、処理を終了する。

【００６６】以上のようにして、判定部３０３における判定処理が行われる。

【００６７】次に、判定部３０４について説明する。

【００６８】判定部３０４は、捕捉したパケットがスパムメールに関連するパケットであるか否かを判定する。具体的には、判定部３０４は、パケット捕捉部３０２から順次渡されるメールヘッダ及びＴＣＰ／ＩＰヘッダを記録しておき、同一の送信元から、所定時間内に、所定数以上のメール・パケットを受信した場合であって、当該メールが転送メールである場合、当該メール・パケットがスパムメールに関連するパケットであると判定する。

【００６９】図６は、判定部３０４の判定処理の流れを示すフローチャートである。

【００７０】同図に示すように、判定部３０４は、まず、パケット捕捉部３０２から渡されるＴＣＰ／ＩＰヘッダに基づいて、同一の送信元から、所定時間内に、所定数以上のメール・パケットを受信しているか否かを判定する（Ｓ６０１）。

【００７１】その結果、同一の送信元から、所定時間内に、所定数以上のメール・パケットを受信していない場合は（Ｓ６０１：ＮＯ）、そのまま処理を終了する。

【００７２】一方、同一の送信元から、所定時間内に、所定数以上のメール・パケットを受信していた場合は（Ｓ６０１：ＹＥＳ）、次に、メールヘッダに基づいて、当該メールが転送メールであるか否かを判定する（Ｓ６０２）。メールが転送メールであるか否かは、例えば、メールヘッダに「Received:」行が所定数以上含まれているか否かで判定する。

【００７３】その結果、転送メールでなかった場合は（Ｓ６０２：ＮＯ）、そのまま処理を終了する。

【００７４】一方、転送メールである場合は（Ｓ６０

２：ＹＥＳ）、捕捉したパケットを拒否すべきパケットと判定し、当該パケットのヘッダ部から、送信元のＩＰアドレスを抽出する（Ｓ６０３）。そして、判定部３０４は、抽出した送信元ＩＰアドレスと、判定部３０４を表す識別子を、フィルタリングルール制御部３０６に渡して（Ｓ６０４）、処理を終了する。

【００７５】以上のようにして、判定部３０４における判定処理が行われる。

【００７６】次に、判定部３０５について説明する。

【００７７】判定部３０５は、捕捉したパケットがポートスキャンに関連するパケットであるか否かを判定する。具体的には、判定部３０５は、通常は使われることがないポート番号のリスト（拒否ポート番号リスト）を保持しており、更に、パケット捕捉部３０２から順次渡されるＴＣＰ／ＩＰヘッダを記録しておき、同一の送信元から、拒否ポート番号リストに含まれる複数（所定数以上）のポートに対するアクセスが、所定の時間内にあった場合、ポートスキャンに関連するパケットであると判定する。

【００７８】図７は、判定部３０５の判定処理の流れを示すフローチャートである。

【００７９】同図に示すように、パケット捕捉部３０２からＴＣＰ／ＩＰヘッダを受け取ると、判定部３０５は、まず、当該パケットが、ポートスキャンに関連するパケットであるか否かを判定する（Ｓ７０１）。

【００８０】その結果、ポートスキャンに関連するパケットでないと判定した場合は（Ｓ７０１：ＮＯ）、そのまま処理を終了する。

【００８１】一方、ポートスキャンに関連するパケットであると判定した場合は（Ｓ７０１：ＹＥＳ）、当該パケットのヘッダ部から、送信元のＩＰアドレスを抽出する（Ｓ７０２）。そして、判定部３０５は、抽出した送信元ＩＰアドレスと、判定部３０５を表す識別子をフィルタリングルール制御部３０６に渡して（Ｓ７０３）、処理を終了する。

【００８２】以上のようにして、判定部３０５における判定処理が行われる。

【００８３】各判定部３０３～３０５から拒否すべき送信元ＩＰアドレス等が渡されると、フィルタリングルール制御部３０６は、当該送信元ＩＰアドレスからのパケットを拒否できるように、パケットフィルタリング部３０１が保持するフィルタリングルールを更新する。

【００８４】また、フィルタリングルール制御部３０６は、保守センターサーバー１０１へ送るため、各判定部３０３～３０５から渡される情報（拒否すべき送信元ＩＰアドレス等）を順次記録しておく。

【００８５】本実施形態においては、フィルタリングルール制御部３０６が追加するフィルタリングルールについて、一時的なものとするか、永久的なものとするかが設定可能である。例えば、スパムメールやポートスキャンについては、一時的に、その送信元からのパケットを拒否するだけで足りる場合があり、一度の不正アクセス等で、永久的に、その送信元からのパケットを拒否するようにすると、不都合な場合がある。

【００８６】このような場合に対応できるようにするため、本実施形態では、各判定部３０３～３０５毎に、各判定部３０３～３０５が拒否すべきと判定した送信元ＩＰアドレスからのパケットを、一時的に拒否するか、永久的に拒否するかを設定できる。そして、一時的拒否に設定された判定部から、拒否ＩＰアドレス等が通知されると、当該拒否ＩＰアドレスに基づいて、フィルタリングルールを追加した時刻を、当該拒否ＩＰアドレスに対応させて記録しておき、追加後、予め決められた時間が経過したら、当該フィルタリングルールを削除する。このような構成とすることで、例えば、基本的には通信を確保したい送信元から、一時的にスパムメールやポートスキャン等があった場合に、当該送信元からのパケットを一時的に拒否して、必要な防御を達成しつつ、基本的には通信を確保したい送信元からのパケットを永久的に拒否する不都合を避けることが可能になる。

【００８７】なお、フィルタリングルール制御部３０６は、フィルタリングルールを削除した時刻も、拒否ＩＰアドレスに対応させて記録しておく。このようにフィルタリングルールを削除した時刻も記録しておくことにより、頻繁に追加・削除が繰り返される場合には、一時的な拒否とされていたものを、永久的な拒否に自動的に変更するように制御することも可能となる。

【００８８】最後に、データ送信部３０７及びデータ受信部３０８について説明する。

【００８９】データ送信部３０７は、必要な情報を保守センターサーバー１０１へ送信するためのものである。保守センターサーバー１０１へ送信される情報としては、フィルタリングルール制御部３０６に保持されている拒否ＩＰアドレス、拒否文字列、フィルタリングルール追加時刻及びフィルタリングルール削除時刻等や、判定部３０３が保持する拒否文字列リストや、ファイアウォール装置１０２の動作モード情報等がある。

【００９０】データ受信部３０８は、保守センターサーバー１０１から送信されてくる拒否パケット識別情報（拒否文字列及び拒否ＩＰアドレス）を受信し、拒否文字列を判定部３０３に渡し、拒否ＩＰアドレスをフィルタリングルール制御部３０６に渡す。

【００９１】ファイアウォール装置１０２は、以上のような構成を有しているので、望まないパケットを検出した場合に、自動的にフィルタリングルールを更新することで必要な防御を自律的に達成すること、及び、保守センターサーバー１０１との間で必要なデータのやり取りを行うこと等が可能となる。

【００９２】次に、保守センターサーバー１０１の詳細について説明する。

【００９３】図８は、保守センターサーバー１０１のハードウェア構成例を示す図である。同図に示すように、保守センターサーバー１０１は、ＣＰＵ８０１と、メインメモリ８０２と、ハードディスクインタフェース部８１０と、ハードディスク装置８１１と、ネットワークインタフェース部８０６とを備える。

【００９４】ＣＰＵ８０１、メインメモリ８０２、ハードディスクインタフェース部８１０、ネットワークインタフェース部８０６は、それぞれ、バス８０８に接続されている。また、ハードディスクインタフェース部８１０には、ハードディスク装置８１１が接続されている。ネットワークインタフェース部８０６は、外部ネットワーク（インターネット１０４）に接続される。

【００９５】ＣＰＵ８０１は、保守センターサーバー１０１が行う各種処理を実行・制御する中央処理装置である。メインメモリ８０２は、ＣＰＵ８０１が利用する各種プログラムやデータを格納する主記憶装置である。ハードディスク装置８１１は、ＣＰＵ８０１が利用するＯＳその他の各種プログラムやデータを格納する補助記録装置である。

【００９６】ハードディスクインタフェース部８１０は、ハードディスク装置８１１とバス８０８との間のデータのやり取りを制御するものである。ネットワークインタフェース部８０６は、外部ネットワークとバス８０８との間のデータのやり取りを制御するものである。

【００９７】図９は、保守センターサーバー１０１のソフトウェア構成例を示す図である。

【００９８】同図に示すように、保守センターサーバー１０１は、データ受信部９０１と、記録部９０２と、統計処理部９０３と、拒否パケット識別情報データベース９０４と、送信データ選択部９０５と、データ送信部９０６とを備える。各部９０１～９０６は、基本的に、ＣＰＵ８０１が、メインメモリ８０２にロードされたプログラムを実行することで実現される。

【００９９】データ受信部９０１は、各ファイアウォール装置１０２から送られてくる情報を受信する。各ファイアウォール装置１０２から送られてくる情報には、各ファイアウォール装置１０２の現在の動作モード情報と、各ファイアウォール装置１０２で拒否すべきと判定したパケットに関する拒否パケット情報（フィルタリングルール制御部３０６が保持する情報）、各ファイアウォール装置１０２が現在使用している拒否文字列リスト（判定部３０３が保持）等が含まれる。

【０１００】各ファイアウォール装置１０２から送られてきた拒否パケット情報は、記録部９０２に記録される。記録部９０２には、複数のファイアウォール装置１０２から送られてくる拒否パケット情報が順次記録される。統計処理部９０３は、記録部９０２に記録された拒否パケット情報を定期的に（例えば、一日一回）統計処理して、複数のファイアウォール装置１０２で共有すべき拒否パケット識別情報を決定し、拒否パケット識別情報データベース９０４に格納する。

【０１０１】図１０は、拒否パケット識別情報データベース９０４の構成例を示す図である。

【０１０２】同図に示すように、本データベース９０４は、「カテゴリ」フィールド１００１と、「データ種」フィールド１００２と、「データ」フィールド１００３と、「原因」フィールド１００４とを備える。

【０１０３】「カテゴリ」フィールド１００１には、カテゴリを識別する識別子（例えば、０００～９９９のいずれか）が格納される。

【０１０４】「データ種」フィールド１００２には、「データ」フィールド１００３に格納されているデータの種類を示す情報が格納される。具体的には、「拒否文字列」であるか、「拒否ＩＰアドレス」であるかを示す情報が格納される。

【０１０５】「データ」フィールド１００３には、「データ種」フィールド１００２に示されたデータの種類に対応して、拒否文字列又は拒否ＩＰアドレスが格納される。

【０１０６】「原因」フィールド１００４には、「データ」フィールドに格納されているＩＰアドレスが、いかなる原因で拒否すべきＩＰアドレスとされているのかを示す情報が格納される。具体的には、「スパムメール」に関連するものとして拒否すべきとされているのか、「ポートスキャン」に関連するものとして拒否すべきとされているのか等を示す情報が格納される。

【０１０７】送信データ選択部９０５は、「カテゴリ」フィールド１００１と「原因」フィールド１００４を使って、各ファイアウォール装置１０２から送られてきた動作モード情報に合致する拒否パケット識別情報を、拒否パケット識別情報データベース９０４から読み出す。そして、必要に応じて、読み出した拒否パケット識別情報と、各ファイアウォール装置１０２から送られてきた拒否パケット情報及び拒否文字列リストとを比較し、両者の差、すなわち、各ファイアウォール装置１０２が有していない拒否パケット識別情報を選択して、データ送信部９０６へ渡す。

【０１０８】データ送信部９０６は、送信データ選択部９０５から渡された拒否パケット識別情報を、データ受信部９０１から渡される送信元情報（送信元ＩＰアドレス等）を使って、今回、拒否パケット情報等を送ってきたファイアウォール装置１０２へ返信する。

【０１０９】なお、保守センターサーバー１０１は、拒否パケット識別情報データベース９０４の「データ」フィールド１００３に含まれているＩＰアドレスを有するホストが稼働（存在）しているか否かを、定期的に調べて、稼働（存在）していないと判断された場合は、拒否パケット識別情報データベース９０４から適宜削除する等、拒否パケット識別情報データベース９０４のメイン

テナンスも行う。

【０１１０】保守センターサーバー１０１は、以上のような構成を有しているので、各ファイアウォール装置１０２との間で必要なデータのやり取りを行うこと等が可能となる。

【０１１１】

【発明の効果】以上詳細に説明したように、本発明によれば、運用するのが容易なパケットフィルタリング型のファイアウォールシステムを提供することができる。

【図面の簡単な説明】

【図１】　本発明によるファイアウォールシステムの全体構成を示す図である。

【図２】　ファイアウォール装置１０２のハードウェア構成例を示す図である。

【図３】　ファイアウォール装置１０２のソフトウェア構成例を示す図である。

【図４】　捕捉パケット記録テーブルの構成例を示す図である。

【図５】　判定部３０３の判定処理の流れを示すフローチャートである。

【図６】　判定部３０４の判定処理の流れを示すフローチャートである。

【図７】　判定部３０５の判定処理の流れを示すフローチャートである。

【図８】　保守センターサーバー１０１のハードウェア構成例を示す図である。

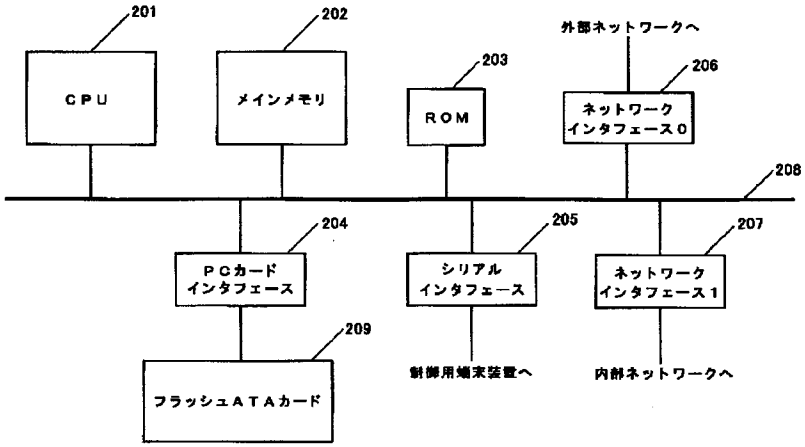
【図９】　保守センターサーバー１０１のソフトウェア構成例を示す図である。

【図１０】　拒否パケット識別情報データベース９０４の構成例を示す図である。

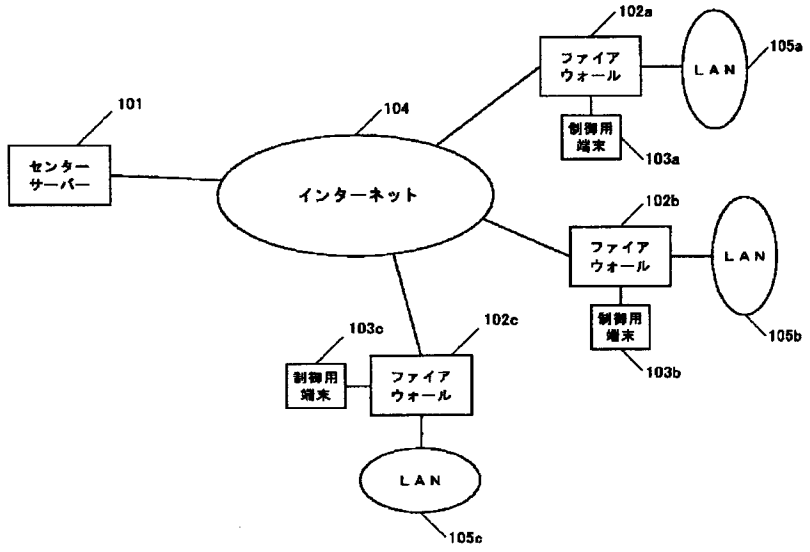
【符号の説明】

＊１０１　保守センターサーバー
１０２ａ～１０２ｃ　ファイアウォール装置
１０３ａ～１０３ｃ　制御用端末装置
１０４　インターネット
１０５ａ～１０５ｃ　内部ネットワーク
２０１　ＣＰＵ
２０２　メインメモリ
２０３　ＲＯＭ
２０４　ＰＣカードインタフェース部
２０５　シリアルインタフェース部
２０６，２０７　ネットワークインタフェース部
２０８　バス
２０９　フラッシュＡＴＡカード
３０１　パケットフィルタリング部
３０２　パケット捕捉部
３０３～３０５　判定部
３０６　フィルタリングルール制御部
３０７　データ送信部
３０８　データ受信部
８０１　ＣＰＵ
８０２　メインメモリ
８０６　ネットワークインタフェース部
８０８　バス
８１０　ハードディスクインタフェース部
８１１　ハードディスク装置
９０１　データ受信部
９０２　記録部
９０３　統計処理部
９０４　拒否パケット識別情報データベース
９０５　送信データ選択部
＊　９０６　データ送信部

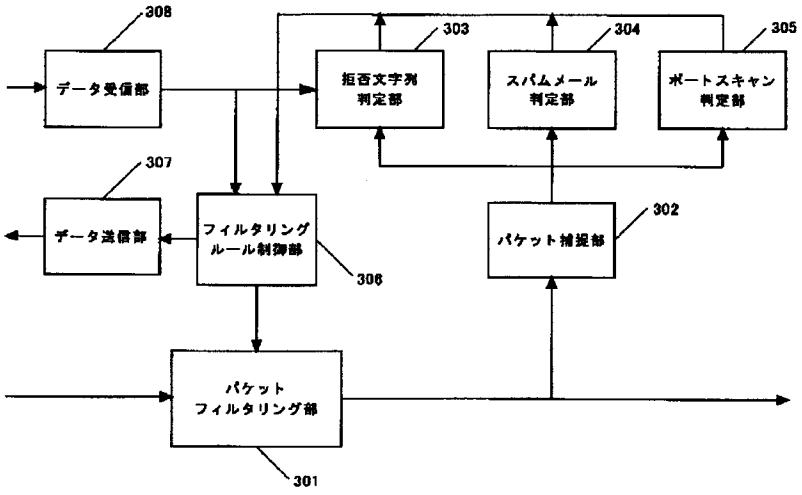
【図２】



【図１】


102a
ファイア
ウォール
LAN
105a
101
104
制御用
端末
103a
センター
サーバー
インターネット
102b
ファイア
ウォール
LAN
制御用
端末
105b
103c
102c
制御用
端末
ファイア
ウォール
103b
LAN
105c

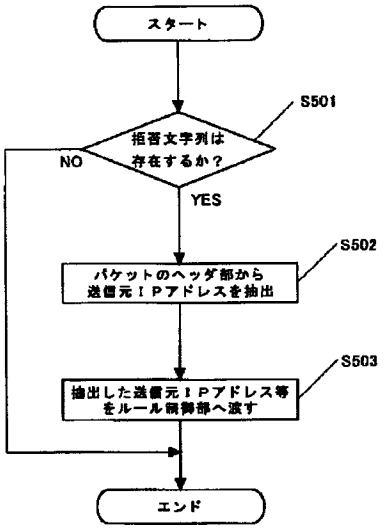
【図３】


308
303
304
305
データ受信部
拒否文字列
判定部
スパムメール
判定部
ポートスキャン
判定部
307
データ送信部
フィルタリング
ルール制御部
306
パケット捕捉部
302
パケット
フィルタリング部
301

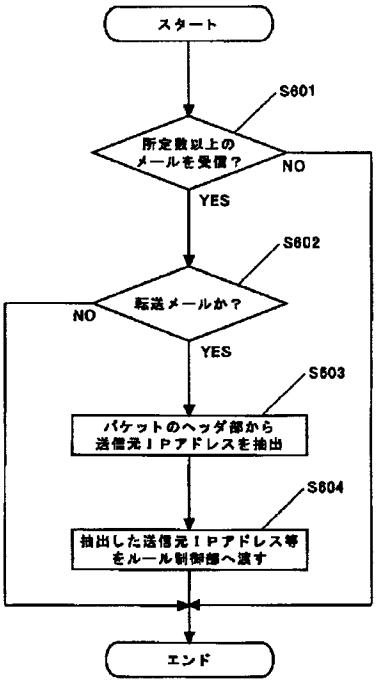
【図４】

401 送信元	402 宛先	403 プロトコル	404 受信時刻
AAA	BBB	UDP	XXX
CCC	DDD	TCP	YYY
EEE	FFF	TCP	ZZZ

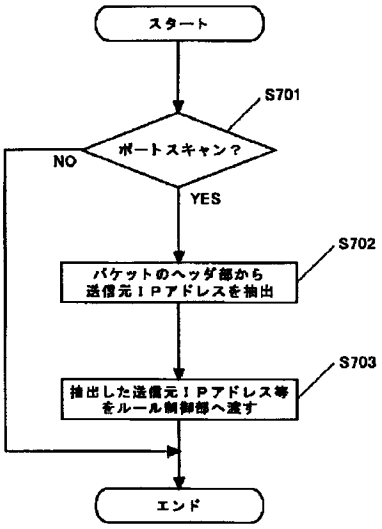
【図５】



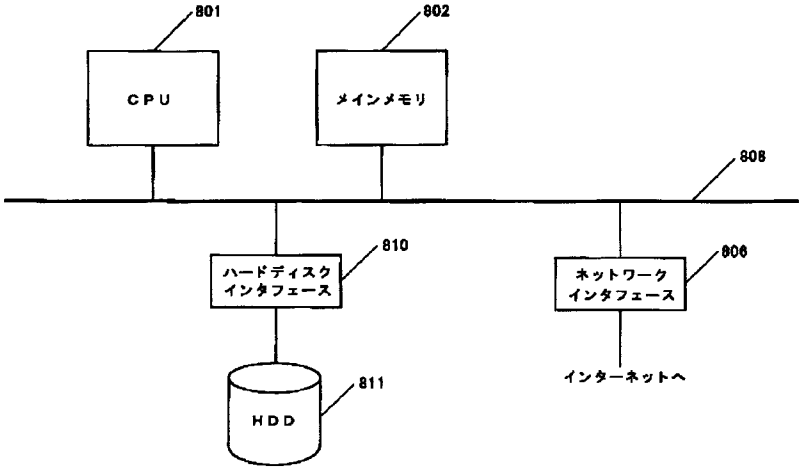
【図６】



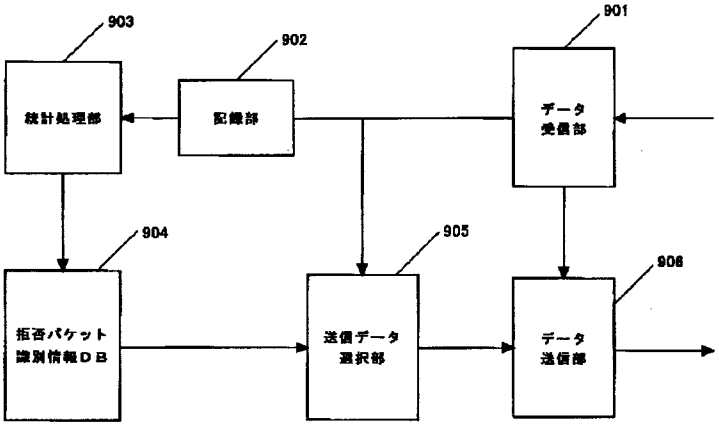
【図７】



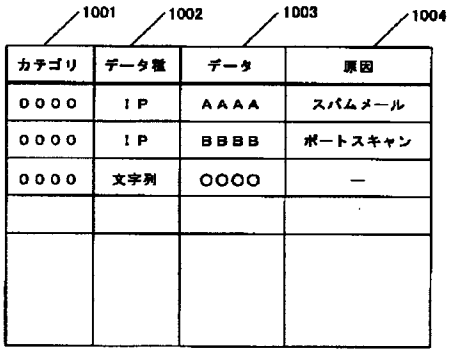
【図８】


801
CPU
802
メインメモリ
808
810
ハードディスク
インタフェース
806
ネットワーク
インタフェース
811
HDD
インターネットへ

【図９】


903
統計処理部
902
記録部
901
データ
受信部
904
拒否パケット
識別情報ＤＢ
905
送信データ
選択部
906
データ
送信部

【図１０】



フロントページの続き

Ｆターム(参考) 5B089 GA04 GA11 JB16 KA17 KB13
MC08
5K030 GA15 HA08 HD08 JA10 KX24
LC14 LC15 MC07